IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Peter V. Radatti and Timothy R. Eliseo

Application Serial No.: 09/800,314

Group Art Unit: 2131

Atty Docket No.: 17-00

Filed: March 6, 2001

Examiner: not yet assigned

For: APPARATUS AND METHODS FOR INTERCEPTING, EXAMINING AND CONTROLLING CODE, DATA AND FILES AND THEIR TRANSFER

PETITION TO MAKE SPECIAL
UNDER 37 C.F.R. § 1.102(d)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant hereby petitions under 37 CFR § 1.102(d) and MPEP 708.02(VIII) that the subject application be accorded special status and advanced in order of examination.

The requirements of 37 C.F.R. § 1.102 and MPEP § 708.02 are fulfilled as follows:

1. A check for the appropriate fee ($130.00) as set forth in 37 C.F.R. §1.17(h) is attached hereto.

2. The patent application filed on March 6, 2001, accorded U.S. Serial No. 09/800,314, as amended by a Preliminary Amendment filed on July 3, 2003, presents Claims 1-13 drawn to a single invention. In the event that restriction is required, an election will be made without traverse.

3. A pre-examination search was made. The classes and subclasses searched were **709/204, 709/217, 709/218, 709/230, 709/231, 709/232, 709/246, 709/250, 713/201, and 714/38.** An Information Disclosure Statement (IDS) is filed concurrently herewith. The listed publications, copies enclosed, represent the results of the search.

4. A copy of each of the cited publications is enclosed for the record.

5. A detailed discussion of the publications follows, pointing out, with particularity as set forth in 37 C.F.R. §§ 1.111(b) and (c), that the claimed subject matter is patentable over the cited publications.

Applicants respectfully submit that all requirements called for by the applicable rules have been fulfilled. Applicants respectfully request early favorable action on this Petition.

Detailed Description of the Cited Art

This detailed description of the related art is submitted as part of the Petition to Make Special pursuant to 37 C.F.R. § 1.102 and MPEP § 708.02. The publications uncovered during the pre-examination search and cited by the Applicants are discussed below.

U.S. PATENTS				
No.	**Patent No.**	**Inventor**	**Date Issued**	**Title**
1	6,421,733	Tso *et al.*	07/16/2002	System for dynamically transcoding data transmitted between computers
2	6,356,951	Gentry, Jr.	03/12/ 2002	System for parsing a packet for conformity with a predetermined protocol using mask and comparison values included in a parsing instruction
3	6,088,803	Tso *et al.*	07/11/2000	System for virus-checking network data during download to a client device
4	5,983,348	Ji	11/09/1999	Computer network malicious code scanner

U.S. PATENTS (cont'd)				
No.	**Patent No.**	**Inventor**	**Date Issued**	**Title**
5	5,916,305	Sikdar *et al.*	06/29/1999	Pattern recognition in data communications using predictive parsers
6	5,889,943	Ji *et al.*	03/30/1999	Apparatus and method for electronic mail virus detection and elimination
7	5,832,208	Chen *et al.*	11/03/1998	Anti-virus agent for use with databases and mail servers
8	5,761,424	Adams *et al.*	06/02/1998	Method and apparatus for programmable filtration and generation of information in packetized communication systems
9	5,623,600	Ji *et al.*	04/22/1997	Virus detection and removal apparatus for computer networks
10	5,586,266	Hershey et. al.	12/17/1996	System and method for adaptive, active monitoring of a serial data stream having a characteristic pattern
11	5,511,163	Lerche *et al.*	04/23/1996	Network adaptor connected to a computer for virus signature recognition in all files on a network
12	5,481,735	Mortensen *et al.*	01/02/1996	Method for modifying packets that meet a particular criteria as the packets pass between two layers in a network
13	5,414,833	Hershey et. al.	05/09/1995	Network security system and method using a parallel finite state machine adaptive, active monitor and responder
14	5,319,776	Hile *et al.*	06/07/1994	In transit detection of computer virus with safeguard
15	5,126,728	Hall	06/30/1992	ADP security device for labeled data

U.S. PUBLISHED PATENT APPLICATIONS				
No.	**Publ. No.**	**Inventor**	**Publ. Date**	**Title**
16	20020004819	Agassy *et al.*	01/10/2002	Device and method for data interception and updating

OTHER DOCUMENTS	
17	Redmond, T., "The Great Anti Virus Crusade", *Windows 2000 Magazine* (April 2001) *pp. 1-4*

Description of the Cited Art

1. U.S. Patent No. 6,421,733 to Tso *et al.*

A system for dynamically transcoding data transmitted between computers is implemented in an apparatus for use in transmitting data between a network server and a network client over a communications link. The apparatus includes a parser coupled to a transcode service provider. The parser is configured to selectively invoke the transcode service provider in response to a predetermined selection criterion.

2. U.S. Patent No. 6,356,951 to Gentry, Jr.

A high performance network interface receives network traffic in the form of packets. The network interface parses one or more headers of a received packet in order to determine whether the packet has been formatted with a pre-selected protocol. If so, one or more efficient enhancements in the processing of a packet may be enabled for the packet. During parsing, header data that may be useful in the processing enhancements may be saved. A packet conforming to one or more of a set of pre-selected protocols may be more completely parsed than a packet not conforming to any of the pre-selected protocols. Instructions for parsing a packet to determine a protocol and to extract useful data are stored in a writeable random-access memory. The instructions may be replaced, modified or supplemented depending upon the composition of network traffic and the protocols selected for enhanced processing. In a parsing instruction executed by a micro-sequencer, a value is extracted from a header and compared to a test value that may be derived from a protocol specification. If the comparison succeeds parsing continues along a first branch; if the comparison succeeds it continues along a second branch. The value extracted from the header may be saved. An offset to a parsing position within the

packet is maintained and updated as the packet is parsed. Values other than those extracted for comparison may also be identified and saved.

3. U.S. Patent No. 6,088,803 to Tso *et al.*

A system for virus checking a data object to be downloaded to a client device is implemented in a method including the steps of retrieving a data object to be downloaded, scanning the data object for a computer virus, and downloading the data object to the client device if no computer virus is detected.

4. U.S. Patent No. 5,983,348 to Ji

A network scanner for security checking of application programs (e.g. Java applets or Active X controls) received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. Static scanning at the HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-post filter instruction sequence or otherwise. The instrumented applet is then transferred to the client (web browser) together with security monitoring code. During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation.

5. U.S. Patent No. 5,916,305 to Sikdar *et al.*

Data communication packets are processed to determine whether they match network protocols using a parser table and a predictive parser. The parser table is encoded from production rules derived from a network protocol definition. Packets comprise data elements each having an offset from the beginning of the packet and a data value. The parser table is indexed by these offsets and data values, each location in the table containing a value indicating whether a data element at the offset and having the data value is a valid element for the network

protocol definition. Once encoded, the parser table is used with the predictive parser which receives data elements of a data packet from a network source. The predictive parser uses the offset and data value of each data element to obtain the encoded value in the parser table. The predictive parser updates a parser stack according to the value from the parser table and the current value of the parser stack. The parser table indicates which offset, value pairs are associated with the end of the data packet or other portion of interest. When the end is reached, the parser stack indicates whether the data packet matched the network protocol definition.

6. U.S. Patent No. 5,889,943 to Ji *et al.*

The detection and elimination of viruses on a computer network is disclosed. An apparatus and method for detecting and eliminating viruses which may be introduced by messages sent through a postal node of an electronic mail system includes polling and retrieval modules in communication with the postal node to determine the presence of unscanned messages and to download data associated with them to a node for treatment by a virus analysis and treatment module.

7. U.S. Patent No. 5,832,208 to Chen *et al.*

A software agent for detecting and removing computer viruses located in attachments to e-mail messages. A client-server computer network includes a server computer and a plurality of client computers. A message system, located at the server computer, controls the distribution of e-mail messages. An anti-virus module, located at the server computer, scans files for viruses. The agent is located at the server computer and provides an interface between the anti-virus module and the message system. The agent can operate both on a real-time basis and at preset period intervals. E-mail messages that are sent internally within the network can be scanned, e.g., Intranet e-mail messages. In addition, e-mail messages received over the Internet can be scanned.

8. U.S. Patent No. 5,761,424 to Adams *et al.*

A method and associated apparatus for automating the filtration and generation of information in a packetized communication system. A filtration table includes entries used in recognizing a valid packet received at a node in a communication system. A mask field in each entry is applied to appropriate fields in the packet (e.g. the ordered set as applied to Fibre Channel communication systems) to determine the validity of the packet with regard to the receiving node. Rules in a field of each entry further qualify the recognition of a received packet (e.g. ordered set) by testing the reception of the packet against other logical rules. Action fields in each record permit definition of actions to be invoked automatically (e.g. automatic adjustment of fill transmissions in Fibre Channel applications) in response to receipt and recognition of a particular packet. The set of packets recognized by the receiving node may be modified by adding, deleting, or modifying the entries in the filtration table. The programmable filtration thereby permits simple modifications to the protocol supported by the receiving node. Programmable generation capabilities of the present invention permit rapid integration of additional packets (e.g. ordered sets) transmitted in response to perceived packets in the receiving node. Programmable parameters in the receiving node permit automatic generation and transmission of packets in accordance with the parameter settings at the time of packet transmission.

9. U.S. Patent No. 5,623,600 to Ji *et al.*

A system for detecting and eliminating viruses on a computer network including a File Transfer Protocol (FTP) proxy server, for controlling the transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system. The FTP proxy server and SMTP proxy server run concurrently with the normal

operation of the system and operate in a manner such that viruses transmitted to or from the network in files and messages are detected before transfer into or from the system. The FTP proxy server and SMTP proxy server scan all incoming and outgoing files and messages, respectively before transfer for viruses and then transfer the files and messages, only if they do not contain any viruses. A method for processing a file before transmission into or from the network includes the steps of: receiving the data transfer command and file name; transferring the file to a system node; performing virus detection on the file; determining whether the file contains any viruses; transferring the file from the system to a recipient node if the file does not contain a virus; and deleting the file if the file contains a virus.

10. U.S. Patent No. 5,586,266 to Hershey et al.

An adaptive, active monitor invention is useful in detecting characteristic data patterns in messages on a high speed data network, such as starting delimiters, tokens, various types of frames, and protocol information. Such serial data streams include serial patterns of binary bits, and can also include serial patterns of multiple state symbols, such as in token ring networks and FDDI networks. The adaptive, active monitor includes two finite state machines (FSM) which are constructed to detect the occurrence of a characteristic data pattern having multiple component bit patterns. A first FSM is the predecessor FSM, and it is configured to detect the first occurring component pattern. A second FSM is called the successor FSM, and it is configured to detect the second occurring component pattern. The first FSM will send a starting signal to the second FSM, when the first FSM has successfully detected the first component pattern. The starting signal initializes the second FSM, to take over the analysis of the portion of the bit stream which follows the first component pattern. If the second FSM successfully detects

the second component pattern, it then outputs a pattern alarm signal, indicating the successful detection of the entire characteristic data pattern.

11. U.S. Patent No. 5,511,163 to Lerche *et al.*

A data processing system comprising a plurality of computers interconnected through a local network, preferably in the form of a ring. The network being connected to a network adapter which is able to receive all information on the network. The network adaptor is connected to a computer which together with the adaptor can perform an assembling and scanning of substantially all files on the network and carry out a recognition of virus signatures. The individual file packets circulation in the network are assembled, said file packets being assembled in a file and scanned for virus signatures. When a virus signature is detected in the file, information is simultaneously provided on the transmitting stations and the receiving stations, whereafter it is possible to transmit the vaccine to the stations in question.

12. U.S. Patent No. 5,481,735 to Mortensen *et al.*

A method and apparatus in a computer system coupled to a network for altering information in said network by the computer system. A process is inserted between two lower layers of the ISO/OSI model. The process then receives a packet from a first layer of the ISO/OSI model, and determines whether a criteria comprising a set of conditions has been determined in the packet. If any of the set of criteria is present in the packet then the packet is transformed into a modified packet according to a predefined action. Then, the modified packet is transmitted to a second layer of the ISO/OSI model. In different embodiments the layers may be either higher or lower relative to one another in order that incoming or outgoing packets be modified. The method may also be performed under control of a user-generated script, or by

remote control from another node. The method may also employ user-generated processes for condition (criteria) checking and/or modifications.

13. U.S. Patent No. 5,414,833 to Hershey et al.

A system and method provide a security agent, consisting of a monitor and a responder, that respond to a detected security event in a data communications network, by producing and transmitting a security alert message to a network security manager. The alert is a security administration action which includes setting a flag in an existing transmitted protocol frame to indicate a security event has occurred. The security agent detects the transmission of infected programs and data across a high-speed communications network. The security agent includes an adaptive, active monitor using finite state machines, that can be dynamically reprogrammed in the event it becomes necessary to dynamically reconfigure it to provide real time detection of the presence of a suspected offending virus.

14. U.S. Patent No. 5,319,776 to Hile *et al.*

Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network. Each character of the incoming data stream is tested using a finite state machine which is capable of testing against multiple search strings representing the signatures of multiple known computer viruses. When a virus is detected the incoming data is prevented from remaining on the destination storage medium. Both hardware and software implementations are envisioned.

15. U.S. Patent No. 5,126,728 to Hall

A data processing security device, attached to computing equipment, inserts labels into a data stream that indicate security controls for the data. The security device may also be configured to detect security labels within a data stream and inhibit the flow of data. It also may

replace data within a data stream if it detects labeled fields which indicate that privacy should be imposed.

16. U.S. Published Patent Application No. 20020004819 to Agassy *et al.*

Apparatus for intercepting data communicated between a sender and a receiver, and conditionally altering that data, the apparatus comprising: an interception unit, capable of intercepting said data, setting information for storing predetermined device settings, access functionality, associated with said interception unit operable to access information within said intercepted data, and a search and replace unit, associated with both said interception unit and said access functionality, for conditionally altering the intercepted data in response to said accessed information and said device settings. The device is useful for dynamically updating web pages and the like and said updating may be made conditional on communication control information such as the identity of an intended recipient as well as data content.

17. Redmond, T., "The Great Anti Virus Crusade", *Windows 2000 Magazine*

The article reviews anti virus products in an Exchange environment. The products appear to utilize API's or dedicated .dll's to access and scan messages.

Description of the Invention

The present invention comprises apparatus and methods for intercepting, examining, and controlling code. The present invention may operate on a single computer system or multiple systems depending on the operating system and other variables. The present invention may, in various embodiments, process, that is, intercept, examine, and/or control any or all code streams in a computer or network. Intercepting, examining and/or controlling code includes but is not limited to monitoring, blocking, logging, quarantining, discarding or transferring code.

Although the present invention can be implemented on various platforms, the preferred embodiments are used in Unix® and various Windows® environments, such as NT, 2000, 95, 98 and Me.

The preferred embodiments monitor transfers from a system using a protocol parser which may be placed on the client system, the server system, or other intermediate system or component. In the especially preferred Unix® embodiments, the protocol parser is a Unix® STREAMS module and driver activated when an application opens a STREAMS device of the proper type. In the especially preferred Windows® NT embodiments, the protocol parser is a WinNT driver activated when an application opens a communications channel.

Analysis of the Cited Art

Claim 1 is representative of aspects of the invention. This claim is reproduced below for the Examiner's convenience.

1. An apparatus for intercepting and processing code on a communications channel comprising:

- a protocol parser; and,

- a proscribed code scanner;

whereby said protocol parser intercepts said code traveling on said channel and transmits said code for review by said proscribed code scanner.

None of the related art known or discovered by Applicants teaches or suggests this apparatus or method.

The two main groups of art Applicant has found involve, separately, anti virus scanners and protocol parsers. As the review below shows, Applicant has been unable to find in the art any teaching, suggestion or disclosure of combining a protocol parser with a proscribed code scanner, as taught by claim 1 of the present invention.

Virus Scan Type Apparatus and/or Methods

U.S. Patent No. 6,088,803 to Tso *et al.*, U.S. Patent No. 5,983,348 to Ji, U.S. Patent No. 5,889,943 to Ji *et al.*, U.S. Patent No. 5,832,208 to Chen *et al.*, U.S. Patent No. 5,623,600 to Ji *et al.*, U.S. Patent No. 5,586,266 to Hershey et al., U.S. Patent No. 5,511,163 to Lerche *et al.*, U.S. Patent No. 5,414,833 to Hershey et al., and U.S. Patent No. 5,319,776 to Hile *et al.* all appear to disclose virus scanning type apparatus and/or methods:

U.S. Patent No. 6,088,803 to Tso *et al.*, discloses a proxy server type of apparatus that retrieves data object(s), and scans the objects prior to their transmission to a client. There appears to be no mention of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,983,348 to Ji discloses a network scanner for security checking of application programs. The scanner is apparently implemented as a HTTP proxy server. There appears to be no mention of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,889,943 to Ji *et al.* discloses a scanner in an electronic mail system. Apparently, a dedicated node is provided for interception of email with an anti virus scanner attached. Again, Applicant is unable to locate anywhere in Ji a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,832,208 to Chen *et al.* discloses an anti-virus module, located at a server computer, which scans files for viruses. Again, Applicant is unable to locate anywhere in Chen a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,623,600 to Ji *et al.* discloses a system for detecting and eliminating viruses on a computer network through two proxy servers -- an File Transfer Protocol (FTP) proxy server and a Simple Mail Transfer Protocol (SMTP) proxy server. Again, Applicant is unable to locate anywhere in Ji a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,586,266 to Hershey et al. discloses an adaptive scanner, which looks for patterns in data streams. The scanner, which operates through a number of finite system machines, operates to detects virus and other signatures, and modifies the stream if desired to warn users, etc. Again, Applicant is unable to locate anywhere in Hershey a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,511,163 to Lerche *et al.* discloses a network adaptor, which is contained with a local area network. The network adapter, along with a computer to which it is connected, performs an assembling and scanning of substantially all files on the network and carry out a recognition of virus signatures. Again, Applicant is unable to locate anywhere in Lerche a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention. Rather, Lerche appears to combine packets into a file before scanning the packets.

U.S. Patent No. 5,414,833 to Hershey et al. discloses an adaptive scanner, which looks for patterns in data streams. The scanner, which operates through a number of finite system machines, operates to detects virus and other signatures. Again, Applicant is unable to locate anywhere in Hershey a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention.

U.S. Patent No. 5,319,776 to Hile et al. discloses a finite state machine for character by character detection of viruses in data in transit between a source medium and a destination

medium, such as between two computer communicating over a telecommunications link or network. Again, Applicant is unable to locate anywhere in Lerche a teaching, suggestion or disclosure of a parser as in claim 1 of the present invention. Rather, Hile appears to scan each character as it is transmitted, rather than packets implemented according to a protocol.

Protocol Parser-Type Apparatus and/or Methods

U.S. Patent No. 6,421,733 to Tso *et al.*, U.S. Patent No. 6,356,951 to Gentry, Jr., U.S. Patent No. 5,916,305 to Sikdar *et al.*, U.S. Patent No. 5,761,424 to Adams *et al.*, U.S. Patent No. 5,481,735 to Mortensen *et al.* and U.S. Published Patent Application No. 20020004819 to Agassy *et al.* all appear to disclose protocol parser-type apparatus and/or methods:

U.S. Patent No. 6,421,733 to Tso *et al.*, U.S. Patent No. 5,761,424 to Adams *et al.*, U.S. Patent No. 5,481,735 to Mortensen *et al.* and U.S. Published Patent Application No. 20020004819 to Agassy *et al.* appear to use parsers to provide manipulation of data transmitted between computers.

U.S. Patent No. 6,356,951 to Gentry, Jr., U.S. Patent No. 5,916,305 to Sikdar *et al.* and U.S. Patent No. 5,761,424 to Adams *et al.* appear to provide parsers to match data packets to protocol templates in order to increase efficiency and/or accuracy of packet processing.

None of these parser related patents appear to disclose scanning the received packets for proscribed code, as claimed in claim 1 of the present invention. Nor is there apparently any teaching, suggestion or disclosure of combining a parser with a proscribed code or any scanner, as in claim 1 of the present invention.

Finally, the article by T. Redmond "The Great Anti Virus Crusade", Windows 2000 Magazine, discloses a specific type of program (linked to an available API or through a dll) rather than any parser as in claim 1 of the present invention.

Accordingly, Applicant submits, insofar as none of the references disclose the elements of claim 1, claim 1 is patentable over the disclosed art. Claims 2-7 have the limitations of claim 1 and so Applicant submits, are also patentable.

Amended Claim 8 (by Preliminary Amendment, copy enclosed) is also representative of aspects of the invention. This claim is reproduced below for the Examiner's convenience.

8. A method for processing code on a communications channel comprising:

- intercepting said code;

- parsing said code;

- scanning said code for the presence of proscribed code; and,

- providing an indicator for the presence of said proscribed code.

None of the related art known or discovered by Applicants teaches or suggests this apparatus or method. As was noted above, any art that discloses scanning appears to do so without parsing, and Applicant is unable to find any reference in the scanning art disclosed herein to parsing code in order to scan. Moreover, any art that discloses parsing appears to do so in the context of manipulation and/or efficiency, and Applicant is unable to find any reference in the parsing art disclosed herein to scanning any parsed code for the presence of proscribed code.

Accordingly, Applicant submits, insofar as none of the references disclose the elements of claim 8, claim 8 is patentable over the disclosed art. Claims 9 - 13 have the limitations of claim 8 and so Applicant submits, are also patentable.

Accordingly, Applicants respectfully request that the Petition to Make Special be granted, and that the application be taken out of turn for examination. Applicants also respectfully request, in light of the detailed description of the related art herein, early consideration and allowance of the solicited claims.

Respectfully submitted,

Date: 7-10-03

Joseph E. Chovanes
Registration No. 33,481
Attorney for Applicants
Suite 329
5 Great Valley Parkway
Malvern, PA, 19355
Tel.: (610) 648-3994
Fax: (610) 648-3997